SEALED

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
MAY - 3 2017
CLERK, U.S. DISTRICT COURT
By _____ Deputy

United States District Court

NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)

2200 Ross Ave, Suite 4900W
Dallas, TX 75201

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: [redacted]

I Emily B. Celeste being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation (FBI) and have reason to believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure) **property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, concerning a violation of Title 18 United States Code, Section(s) 1343, 1346, 666, 371 and 1956. The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT EMILY B. CELESTE).
(Continued on the attached sheet and made a part hereof. XX Yes __ No

Emily B. Celeste
Signature of Affiant
Emily B. Celeste
Special Agent, FBI

Sworn to before me, and subscribed in my presence

May 3, 2017 at 4:46 p.m. **at Dallas, Texas**
Date and Time Issued **City and State**

RENEE HARRIS TOLIVER
United States Magistrate Judge
Name and Title of Judicial Officer

Renee Harris Toliver
Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Emily B. Celeste, a Special Agent (SA) with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed in this capacity since November 2012. I am currently assigned to the FBI's Dallas Division on the Public Corruption Squad. Previously, I was assigned to the FBI Birmingham Division's Cyber Crime Squad in Birmingham, Alabama. I have participated in all of the normal methods of investigation, including but not limited to the use of electronic surveillance, physical surveillance, subject and witness interviews, search warrants, confidential informants, pen registers, and undercover operations. As a Special Agent of the FBI, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. The statements in this affidavit are based on my investigation of this case, information provided by other Special Agents of the FBI, including Special Agents Phillip Stevenson and Erik Tighe, analysis of bank records, examination of real estate documents, examination of public records, and examination of e-mail records regarding business transactions between the subjects discussed herein. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I

have set forth only the facts that I believe are necessary to establish the existence of probable cause to support the issuance of a search warrant for the location further described herein.

STATUTORY VIOLATIONS

3. As a result of my participation in this investigation and information I learned from Special Agents Phillip Stevenson and Erik Tighe, I am familiar with the circumstances surrounding the facts and offenses described in this Affidavit. On this basis, I allege that the information in this Affidavit establishes probable cause to believe that:

   a. Ricky Dale Sorrells (Sorrells), Superintendent at Dallas County Schools (DCS), and Robert Carl Leonard, Jr. (Leonard), President of Force Multiplier Solutions (FXS), have committed violations of Title 18, United States Code, Section 1343 & 1346 (Wire Fraud), Section 371 (Conspiracy), and Section 1956 (Money Laundering) by devising and implementing an ongoing scheme to defraud DCS and taxpayers by the misappropriation of taxpayer and Federal school funds to a private business entity (FXS) through the payment of kickbacks to government officials for official actions taken regarding contracts with FXS and to pass laws to benefit FXS, making false representations or purposeful omissions to DCS and the public by failing to disclose material facts which were harmful to DCS, and establishing shell companies and accounts that were intentionally created to conceal and disguise the source of the proceeds transferred from the vendor (FXS) to the government official (Sorrells).

b. Sorrells, acting in his official position as Superintendent of DCS, did knowingly and willfully conspire with the owner (Leonard) of a vendor (FXS) to embezzle funds awarded by DCS to FXS as a direct result of a contract created and entered into by Sorrells and Leonard as authoritative representatives of their respective employers. Upon receiving payments from DCS for services rendered, FXS would transfer funds through the Fedwire Funds Transfer System to various sources including bank accounts established by Leonard that were used primarily to pay Sorrells' credit card account balances and outstanding loans; bank accounts for businesses that conducted legitimate business but also served to "pass through" funds from Leonard to Sorrells; and bank accounts established seemingly for the sole purpose of adding a layer of protection to conceal or disguise that Leonard was paying Sorrells kickbacks from the money FXS received from DCS.

c. There exists probable cause to believe evidence of the above offenses will be found at the location of Leonard's employment, FXS. The address is as follows:

i. 2200 Ross Ave, Suite 4900W, Dallas, TX 75201

INVESTIGATION OVERVIEW AND BACKGROUND

4. Dallas County Schools (DCS) is an intermediate government agency that serves Dallas County's 12 independent school districts in North Texas. DCS's primary responsibility is the operation of its bus system, which transports approximately 75,000 children to and

from school each day, making DCS the 4th largest pupil transportation organization in the country[1].

5. Force Multiplier Solutions (FXS), headquartered in Dallas, is a full-service technology company that outfits buses with cameras and on-board operating systems for the student transit and public transit industries. FXS was originally incorporated as ONGO Live in Louisiana in 2004, and was primarily used on buses and streetcars to record activity for security purposes. In 2007, ONGO Live began operating on school buses so municipalities or other government entities could issue citations to drivers illegally passing school buses when the "stop arm" was engaged. ONGO Live rebranded in 2011 as FXS, and began operating in Texas when the company moved to Dallas. A sworn peace officer that works for the county where the stop-arm violation occurred is typically responsible for reviewing video footage and issuing a citation, however, some school districts outside Dallas County have chosen to give officials working for Dallas County the authority to review and issue citations for their school districts[2].

6. In 2008, DCS issued a Request for Proposal (RFP) to find a vendor that could replace existing technology on DCS buses, and also help DCS deploy a digital audio/video recording solution that would be upgradable in the future. A growing trend in the pupil transportation industry at this time was the ability to issue citations to drivers that illegally passed a school bus once the stop arm was engaged through the use of video

[1] Dallas County Transportation Department, 2017, http://www.dcschools.com/departments/transportation-department/.
[2] "Ethical questions raised by San Marcos school bus camera tickets," March 1, 2015, http://www.mystatesman.com/news/local-education/ethical-questions-raised-san-marcos-school-bus-camera-tickets/3pwo95uVEoXFBQumvqYw0K/.

monitoring systems. The standard practice for similar stop arm camera programs was for the contractor to put cameras on 20-30% of the stop arms on the buses that traveled routes with the most safety violations free of charge, then share a percentage of the fines levied with the school district. DCS' request was unique in that DCS wanted to outfit all 1900 of their buses with the technology to record and monitor via audio/video solutions and purchase the equipment to do so outright. Due to the unique and unprecedented nature of the RFP, FXS was the only company to reply to the proposal. AT&T phone records show Sorrells and Leonard had at least 20 contacts between January 1, 2009 and July 15, 2009, the date when the vendor was selected. This includes a 45-minute phone call between Leonard's cell phone and Sorrells' home phone that began at approximately midnight on July 3, 2009.

7. In July 2009, DCS awarded the contract to FXS, the only company who submitted a bid to the unusual request for proposal. DCS agreed to purchase all equipment from FXS, after which FXS would install the equipment and software, create an operations center, and oversee all remote and on-site maintenance required to sustain the school bus monitoring systems. In September 2011, DCS and FXS officially entered into a one-year contract that provided both entities the capability of extending the contract another five years. On November 8, 2011, DCS remitted its initial purchase order worth approximately $6 million as an advanced partial payment to FXS. This was followed up on November 9, 2011, by an initial payment by DCS via check to FXS of approximately $2 million.

8. In July 2012, DCS and FXS agreed to extend their contract for the full five years outlined in the initial agreement. The exact financial terms of the contracts signed between DCS and FXS are unknown since the contracts do not explicitly state the financial obligation to which DCS is agreeing. Furthermore, DCS board meeting minutes and budgets often lack documentation detailing contracts that are signed between DCS and FXS. For example, there is no mention in the school board minutes of the RFP awarded on July 15, 2009 to FXS for the stop-arm camera program, or for the $6 million purchase order issued by DCS to FXS. In 2014, DCS did provide some details as to the stated purpose of bonds they issued, most of which included expenditures for "equipment technology on buses." The bonds issued that cover this cost are detailed as follows:

    a. Series 2012, Issued January 1, 2012, $26,570,000
    b. Series 2012-A, Issued June 15, 2012, $20,890,000
    c. Series 2012-B, Issued November 15, 2012, $18,185,000
    d. Series 2013, Issued June 15, 2013, $10,755,000
    e. Series 2014, Issued April 15, 2014, $12,255,000
    f. Series 2014, Issued April 15, 2014, $4,045,000

9. Despite little return on its initial agreement, DCS, in October 2012, agreed to purchase the rights to FXS' "BusGuard" technology for the purposes of marketing and selling FXS' product to school districts throughout the United States. The purchasing price for the rights to be the only vendor of the technology was approximately $25 million. This

additional debt issued by DCS brought the total amount of their contract with FXS to approximately $70 million.[3]

PROBABLE CAUSE

A. Leonard's payments to Sorrells through Allegro

10. In March 2011, around the time DCS and FXS were negotiating the contract to outfit DCS buses with FXS' technology, Margaret Allegro Sorrells (Margaret), wife of Ricky Dale Sorrells, opened a Business Checking account at Wells Fargo Bank (Wells Fargo) for a business called Allegro Research and Consulting (Allegro). Margaret was the only signer on the account and was listed as the owner of Allegro, the location of which was 8539 Forest Hills Blvd, Dallas, TX 75218, the residence of Rick and Margaret Sorrells. Although Margaret's personal listed mailing address on the signature documents for the account was 6158 Chesley Ln, Dallas, TX 75214, available deed records show that Rick and Margaret sold that property in August 2005 and have resided at the Forest Hills address since March 2005, and have also listed the address on Forest Hills Blvd. as their primary residence.

11. According to documents drafted and signed to establish Allegro Research and Consulting's (Allegro) bank account at Wells Fargo, Allegro is in the Professional, Scientific, and Technical Services industry. The funding to open Allegro, and several payments thereafter, originated from Leonard. On March 23, 2011, Leonard wrote a

[3] Since the issued bonded debt is not tied to specific expenditures within particular accounts, the exact amount of funds DCS allocated to pay FXS is unknown at this time. Based on a review of multiple FXS bank accounts, agents believe DCS has paid FXS approximately $50 million, and owes FXS approximately $20 million in future payments.

check out of the ONGO Live account at Regions Bank 5126 for $16,000 to [redacted]. The check was deposited into the Whitney Bank account for [redacted], ending in 2657, on March 23, 2011. On March 28, 2011, [redacted] wrote a check for $15,000 from Whitney Bank account 2657 to Margaret's Allegro Wells Fargo account 4586 that was deposited on April 1, 2011. This was the initial deposit Margaret used to establish her 4586 business account at Wells Fargo. On May 26, 2011, [redacted] deposited a second check from ONGO's 5126 Regions account for $10,000 that was written on May 26, 2011 and signed by Elizabeth Michener (Michener), Leonard's assistant. That same day, [redacted] wrote Margaret a check for $10,000 that was deposited into the Allegro Wells Fargo account 4586 on May 31, 2011. On July 20, 2011, [redacted] deposited a third check, this time from Busguard LLC, a subsidiary of FXS, for $15,500, which was written on July 20, 2011 from Busguard's Regions 9791 account and signed by Michener. On May 21, 2011, [redacted] wrote a check to Margaret for $15,000 – which was deposited into the Wells Fargo Allegro account 4586 on July 25, 2011 – and a check to himself for $500, the memo line of which stated "Allegro lgl fee," which was deposited into [redacted]' account at Central Progressive Bank in Mandeville, LA, on July 22, 2011. [redacted] deposited a fourth check, again from Busguard, for $10,000 on September 2, 2011, which was written and signed on September 1, 2011 by Michener. On September 6, 2011, [redacted] wrote Margaret a check for $10,000, which Margaret deposited to the 4586 Wells Fargo Allegro account on September 9, 2011.

12. The total amount of funds deposited into the 4586 Allegro checking account was approximately $65,000 – $50,000 of which originated from FXS, ONGO, and Busguard – companies which Leonard owns. Every check that was written by [redacted] and deposited into the 4586 Allegro account was directly preceded by a check of the exact, or similar, amount made out to [redacted] from companies associated with Leonard. There were no checks or deposits into the 4586 Allegro account that did not originate from Leonard's businesses.

13. The address listed for [redacted] on the checks written to Allegro was [redacted]. This is the same address [redacted] provided when he incorporated ONGO Live in Louisiana in 2004. When ONGO/FXS established accounts at the Bank of New Orleans in 2011, [redacted] updated his address to [redacted], which was the same address provided by Leonard, and was the address for ONGO Live at the time. Additionally, [redacted] is the registered agent and co-signer on several of Leonard's Bank of New Orleans business and personal accounts. Accordingly, [redacted] had a connection to FXS, ONGO, and Busguard during the time [redacted] was writing checks to Margaret Sorrells' business.

B. Leonard's payments to Sorrells through Photon

14. On December 2, 2012, Rick and Margaret Sorrells registered a business called Photon IT and Product Development, Inc. (Photon) through the state of Texas using their home address of 8539 Forest Hills Blvd. On December 4, 2012, Rick and Margaret established an account at JPMC for Photon (3560). On December 7, 2012, FXS wired $300,000 from

its operating account at the Bank of New Orleans, account 5238, to [redacted]' 2657 Whitney Bank account, the same account covered in the previous section. Three days later, on December 10, 2012, [redacted] wired $300,000 from Whitney Bank account 2657 to Photon's 3560 bank account at JPMC.

15. On December 19, 2012, FXS wired $200,000 from its 5238 Bank of New Orleans account to an unknown receiver. That same day, [redacted] received a $200,000 wire transfer that originated from the Bank of New Orleans and passed through the Federal Home Loan Bank of Dallas (FHLBD). Based on the date, the specific amount of funds wired, and the payment history between FXS/ONGO/Busguard and Richard [redacted], agents have reason to believe the $200,000 that originated from FXS' 5238 Bank of New Orleans account is the same money that [redacted] received into his 2657 Whitney Bank account. Two days later, on December 21, 2012, [redacted] wired $200,000 from the 2657 Whitney Bank account to Photon's 3560 JPMC account. Furthermore, on April 3, 2013, FXS wired $250,000 from its 6524 Bank of America account to [redacted]' 2657 Whitney Bank account. [redacted] then wrote a check from his 2657 Whitney Bank account on April 4, 2013, that was payable to Photon and deposited into Photon's 3560 JPMC account on April 5, 2013.

16. The source of the $1.6 million deposited into Photon's 3560 JPMC account came from [redacted], Elf Investments, and Sreig International (Sreig), Rick and Margaret's other home business. [redacted] and Elf Investments were responsible for $1.5 million in deposits, and the other $100,000 in deposits came from Sreig. The wire transfers and checks from Elf Investments were originated by Slater Swartwood. During the time of

these transactions, both Slater Swartwood Sr. and Slater Swartwood Jr. worked for FXS, according to pay stubs and telephone records.

17. Sreig International (Sreig), the other source of funds for Photon, received $630,000 worth of deposits from July 2015 to June 2016. Anrock Realty Services, LLC was responsible for $600,000 of the funds deposited into Sreig's 7802 JPMC account. According to Louisiana State Business Entity records, Anrock Realty Services was created in January 2015 by Slater Swartwood. According to Whitney Bank subpoena returns, Slater Swartwood, Jr. is the account owner for a company called Anrock Funding, LLC. According to Slater Swartwood Jr's LinkedIn social media page, he has worked for FXS since 2010 as the director of marketing. According to AT&T telephone records and checks written by Leonard from the FXS 0725 Bank of New Orleans account, Slater Swartwood, Sr. has also been employed by FXS since approximately 2011.

C. Leonard's Payments to Sorrells through Slater Swartwood

18. On November 7, 2011, Slater Swartwood, Sr. opened a free smart business checking account with Whitney Bank for a business called Cambridge Realty Group, LLC (Cambridge), ending in 5608. Swartwood was the only signer on the account.

19. On November 16, 2011, at approximately 10AM, the Ongo Live account ending in 0325 held at Bank of New Orleans wired the Cambridge 5608 account $220,000. At approximately 1:45 PM that same day, Swartwood wired $200,000 from the Cambridge 5608 account to Sorrells' personal JPMC account ending in 1664.

20. On December 1, 2011, the Ongo Live account ending in 5126 held at Regions Bank wired $50,000 to the Cambridge 5608 account. On December 2, 2011, Swartwood wrote

a check for $50,000 out of the Cambridge 5608 account, payable to Rick Sorrells, which was cashed on December 6, 2011 into the JPMC 1664 account. The memo line on the check read "Loan."

21. On March 14, 2012, the Cambridge 5608 account received a wire transfer in the amount of $31,000 that was sent through the Federal Home Loan Bank of Dallas. Although the transaction did not show an exact originator, records obtained via Federal Grand Jury Subpoena reveal that Force Multiplier Solutions wired $31,000 out of their 0725 account to an unknown party on March 14, 2012. Based on the specific date and unique amount, combined with a similar pattern discovered through a review of obtained records, agents have reason to believe FXS transferred $31,000 to Cambridge on March 14, 2012. On March 15, 2012, Cambridge 5608 transferred $31,000 to Sorrells' JPMC 1664 account.

22. The remaining funds in the Cambridge 5608 account were dispersed amongst Swartwood's wife (Kathryn), daughter (Heather Loeb), and Elf Investments – another company Swartwood used to transmit money obtained from Leonard to Sorrells between March 15, 2012, and the time the Cambridge 5608 was closed, approximately June 19, 2012.

D. Leonard pays Sorrells' credit card debt

23. On April 14, 2014, Robert Leonard opened a checking account at JPMC entitled "Robert Carl 2, Inc.," ending in 0039, which was opened with a $100 check from FXS' 0574 account held at the Bank of New Orleans (BNO). On May 21, 2014, FXS transferred $25,000 into JPMC 0039, and again on June 9, 2014, FXS transferred $200,000 into JPMC 0039 – both transfers coming from the BNO FXS account 0574.

On June 11, 2014, Robert Leonard wrote two checks, one to American Express (AMEX) and one to Chase Card Services (JPMC credit card) for the amounts of $16,000 and $14,000, respectively. On the memo lines of the checks were the account numbers for which the checks were to be deposited, 23007 and 9700, respectively. Both AMEX account 23007 and JPMC account 9700 belong to Rick Sorrells. On June 24, 2014, Leonard again wrote a check payable to Sorrells' AMEX account 23007 for the amount of $21,500. Between June 18 and 26, 2014, Leonard transferred $170,000 from JPMC 0039 to his personal account held at JPMC, account number 3128, bringing the amount left in the "Robert Carl 2, Inc." (JPMC 0039) to under $4,000. After nine ATM withdrawals, all in the amount of $400, there was $13 left in the JPMC 0039 before FXS transferred $90,000 on November 10, 2014 from its Bank of America (BOA) (2057) to the JPMC 0039 account. On November 6, 2014, Leonard wrote a check for $22,000 from JPMC 0039 to Sorrells' JPMC 9700 credit card, which was posted on November 14, 2014. Again on November 7, 2014, Leonard wrote a check from the JPMC 0039 to Sorrells' 23007 American Express credit card for $63,000, which was posted on November 12, 2014. Aside from a $1,500 withdraw and a $3,000 transfer from Leonard's "Robert Carl 2, Inc." account at JPMC (0039), no other activity was recorded in this account besides payments to Sorrells' credit card debt. All checks paid to Sorrells' credit card account have been corroborated by obtaining Sorrells' account documents at both JPMC and AMEX through Federal Grand Jury Subpoenas.

24. On March 5, 2014, FXS wrote a check from its BNO account for $18,393.56 payable to Sorrells' AMEX account 23007. On April 9, 2014, FXS wrote two checks in the amount

of $11,480.57 and $21,617.21. The first check was made payable to Sorrells' AMEX account 23007, while the check written to "Card Member Services" had "Ricky D. Sorrells" written on the memo line. These checks differ from the other checks discussed in that the signature is identifiable with that of Elizabeth Michener, Leonard's secretary at FXS, who has signature authority on almost all Leonard's bank accounts.

E. Leonard pays Sorrells' loans

25. In or around August 2004, Rick Sorrells opened, or assisted with the opening of, an account with Sallie Mae, presumably for the purpose of obtaining a student loan. According to Transunion, Equifax, and Experian reports obtained through a Federal Grand Jury Subpoena, the loan was for $20,000. In September of 2004, Sorrells obtained a second loan from Sallie Mae in the amount of $21,000. According to Sorrells' personal 1664 JPMC account, Sorrells made regular payments of approximately $100 per month on these loans until the loans were paid in full in May of 2013 and April of 2014 by FXS. On April 9, 2014, FXS wrote a check from the BNO 0725 account that was payable to Sallie Mae in the amount of $19,215.17. On the memo line of that check from FXS was the account number 9336856952. According to the Transunion, Equifax, and Experian reports, this is the account number associated with both of Rick Sorrells' loans.

F. Communications between Leonard and Sorrells

26. Between April 4, 2011 and June 16, 2016, Sorrells has received approximately $2.7 million in wire transfers that have originated from Leonard's business and personal accounts at multiple banks. Additionally, Sorrells has received approximately $250,000 through loan and credit card payoffs from Leonard. Sorrells and Leonard also

communicated with one another via home phones and cell phones before, during, and after contract negotiations and agreements between DCS and FXS, totaling approximately 1,000 documented contacts between January 1, 2009 and December 27, 2016, according to toll records provided by AT&T Wireless. 40. Per documents obtained via a public information request and a review of signature documents provided by banks subpoenaed during this investigation, along with information corroborated through this investigations, Sorrells, Leonard, and Swartwood, Sr. also communicated through the use of personal and professional electronic mail (e-mail) accounts, which are detailed as follows: rsorrells@dcschoolds.com, ricksorrells@sbcglobal.net, bob.leonard@busguard.net, robert.leonard@fxsinc.com, and cgslater@gmail.com.

G. Conversations regarding bribe cover-up scheme

27. On multiple occasions, Sorrells had conversations with Leonard and Swartwood regarding ways to make bribe payments from Leonard through Swartwood to Sorrells appear legitimate, including the following:

a. On March 11, 2017, Swartwood told Sorrells that Sorrells needed to get rid of any references to payments Sorrells received under the guise of "consulting fees," and that all monies Sorrells received would be tied into the "note". The reference to this "note" is how Leonard, Sorrells, and Swartwood have attempted to disguise the money Sorrells received, which, as Swartwood stated, originated from Leonard and FXS.

b. On March 13, 2017, Leonard also indicated that Leonard had talked with Swartwood, and the two decided their story would be that Sorrells received money

as a personal loan during which Sorrells used his real estate properties as collateral.

c. During a meeting on March 24, 2017, Swartwood provided Sorrells an "updated" version of Sorrells' note, which updated the date upon which Sorrells' payments on the note would begin. The note also stated that Sorrells' loans originated from FXS and were due to Leonard, who was the bearer of the note.

d. During a meeting with Leonard on March 25, 2017, Leonard took the note Sorrells received from Swartwood because Leonard did not want his name on the note as the bearer of Sorrells' loan. Several days later, Swartwood sent Sorrells an updated version of the note, which had FXS and Leonard's name replaced with the phrase "bearer." Additionally, during the meeting between Sorrells and Leonard on March 25, 2017, Leonard advised Sorrells to obtain a "burn" phone so the two could have more candid conversations that would be untraceable.

H. Documentary and electronic records

28. Based on my training, experience, knowledge and participation in this and other criminal investigations, and accumulated knowledge from consultations with other law enforcement agents, I also know and contend that the following traits are common practices of offenders involved in various types of fraud:

a. fraud is frequently a continuing activity over many months and even years;

b. offenders who commit fraud keep records of their illegal activities for a lengthy period of time, even extending substantially beyond the time during which

they actually produce, market, sell, and profit from their crimes;

c. offenders who commit fraud commonly maintain hard copy and computer files, books, records, receipts, notes, ledgers, journals, diaries, address books, and other sundry materials, and papers relating to their crimes; and

d. offenders who commit fraud often possess evidence, fruits, and instrumentalities relating to such offenses in their places of business, including home offices.

29. I am aware that people frequently use both business and personal cellular telephones (commonly called cell phones) for personal and professional communications and purposes. Many cell phones have advanced capabilities, including: Internet browsing, text and e-mail, photography and video storage, notes, calendars, and data file storage. I am also aware, through training and experience, that people use cell phones to communicate with each other via voice, direct connect, text message, and e-mail; store valuable data such as names, and addresses; obtain and store directions and maps; search the Internet and capture audio, image, and video files.

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the TARGET PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive (including a server, such as an email server) or other storage media, including "smart" cellular telephones. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer or storage medium is found on the TARGET PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete

this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, including e-mails and spreadsheets, I am aware that computer equipment was used to generate, store, and print documents used in the fraud scheme described herein. There is reason to believe that there is a computer system, including a computer network, local computers, and e-mail server, currently located on the TARGET

I. Premises

32. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the

computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries,

logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying

for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. I understand that FXS is a functioning company that has on-going business operations. The seizure of FXS' computers may limit FXS' ability to conduct its on-going business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, agents or their qualified analysts will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of FXS so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of FXS' legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it as soon as is practicable.

CONCLUSION

36. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that Ricky Dale Sorrells and Robert Leonard, knowingly and intentionally conspired and agreed with each other to devise a scheme and

artifice to defraud Dallas County Schools and to obtain money from Dallas County Schools by means of official contract obtained in part by kickbacks to influence government officials for the contract for the purposes of executing such scheme and artifice, to use wire communications in interstate commerce, contrary to Title 18, United States Code, Sections 1343 & 1346, and to hide the source of funds through the establishment of shell companies created for the sole purpose of Sorrells receiving funds that were originated by Leonard and were layered through multiple businesses. Additionally, there is probable cause to believe that evidence of these criminal offenses is located in the location described above, and this evidence, which is listed in Attachment A to this affidavit and which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offense.

Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment A.

Emily B. Celeste
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 30th day of May, 2017.

RENEE H. TOLIVER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

Property is located at 2200 Ross Ave, Suite 4900W, Dallas, TX 75201, which is a fifty-five (55) story office building located at the southeast corner of the intersection of Ross Avenue and North Pearl Street. The business to be searched is on the 49th floor of the building and there is an attached parking lot as well as underground parking. The building is tan with tall glass window panes, and the main entrance is located on the southeast side of the building. The names "Chase" and "Deloitte" are displayed on the outside of the north side of the building.

Attachment B

I. Any and all records, documents, files, or materials described in Section I, paragraphs A-G and Section II A-C, in whatever form, that constitute evidence, instrumentalities, or

fruits of a violation of 18 U.S.C. § 1343 & 1346 (Wire Fraud), 18 U.S.C. § 371 (Conspiracy), and 18 U.S.C. § 1956 (Money Laundering) , relating to any one or more of the following entities or their principles, officers, employees, and agents: Ricky Dale Sorrells, Robert Leonard, Force Multiplier Solutions, Dallas County Schools.

A. Records, including electronic communication (i.e., e-mail, text message), concerning or relating to any promise to pay a monetary obligation, including but not limited to open or closed loans, notes, promissory notes, mortgages, mortgage notes, negotiable instruments, letters of credit or any other credit facilities, deeds of trust or other security instruments, loan agreements, participation agreements, loan applications (whether pending, accepted, or rejected), correspondence, checks or deposit items representing the disbursement of principal, collateral ledgers, guarantees, cash flow analysis and projection, interest rate analysis, blended rate analysis, pro formas, loan narratives, appraisals, absorptions, audits, certifications, and loan assignments, modifications, amendments, or terminations;

B. Records, including electronic communication (i.e., e-mail, text message) relating to or concerning invoices, receipts, statements, cancelled checks, general ledgers, trial balances, spreadsheets, correspondence with creditors, credit card transactions, payroll transactions, loans, cash flow analysis, cash flow projection, pro formas, loan narratives, appraisals, collateral, financial analysis, absorptions, audits, certifications, and drafts, filings, and correspondence with the United States Securities and Exchange Commission (SEC);

C. Memoranda, notes, files, videotapes, audiotapes, agendas, and other documents, including electronic communication (i.e., e-mail, text message), relating to any meeting of Sorrells, Leonard, and government officials relating to Dallas County Schools.

D. Records, including electronic communication (i.e., e-mail, text message), relating to or concerning any contracts involving the above-listed entities and third party brokers;

E. Personnel files relating to or concerning any of the executives, officers, employees, and agents of Dallas County Schools and Force Multiplier Solutions.

F. Records, including electronic communication (i.e., e-mail, text message), relating to or concerning any open or closed bank account (whether savings, checking, or other type of account), such records to include periodic account statements, corporate resolutions, partnership agreements, customer ledgers, income tax returns, deposit tickets, cancelled checks, signature cards, account opening documents, and any and all correspondence;

G. Other bank records, including money orders, cashier's checks, and drafts, with application or requisition forms, certified checks, wire transfers, insurance records, safe deposit box records, or copies of any negotiable instruments cashed or paid by the bank without entry to any depository account.

II. Computers and computer related evidence, as follows:

A. Any computer, cellular telephone, computer system and related peripherals including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

B. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, "chat," instant messaging logs, photographs, and correspondence; communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission.

C. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;